

# NON-WIEFERICH PRIMES IN NUMBER FIELDS AND *ABC* CONJECTURE

SRINIVAS KOTYADA AND SUBRAMANI MUTHUKRISHNAN

**ABSTRACT.** Let  $K/\mathbb{Q}$  be an algebraic number field with ring of integers  $\mathcal{O}_K$ . We show that there are infinitely many non-Wieferich primes with respect to certain units in  $\mathcal{O}_K$ , assuming *abc* conjecture for number fields.

## 1. INTRODUCTION

An odd rational prime  $p$  is called Wieferich prime if

$$2^{p-1} \equiv 1 \pmod{p^2}. \quad (1)$$

A. Wieferich [1] proved that if an odd prime  $p$  is non-Wieferich prime, i.e.,  $p$  satisfies

$$2^{p-1} \not\equiv 1 \pmod{p^2},$$

then there are no integer solutions to the Fermat equation  $x^p + y^p = z^p$ , with  $p \nmid xyz$ . The known Wieferich primes are 1093 and 3511 and according to the PrimeGrid project [10], these are the only Wieferich primes less than  $17 \times 10^{15}$ . One of the unsolved problems in this area of research is to determine whether the number of Wieferich or non-Wieferich primes is finite or infinite? Instead of the base 2 if we take any base  $a$ , then  $p$  is said to be a Wieferich prime with respect to the base  $a$  if

$$a^{p-1} \equiv 1 \pmod{p^2}, \quad (2)$$

and if the congruence (2) does not hold then we shall say that  $p$  is non-Wieferich prime to the base  $a$ . Under the famous *abc* conjecture (defined below), J. H. Silverman [2] proved that given any integer  $a$ , there are infinitely many non-Wieferich primes to the base  $a$ . He established this result by showing that for any fixed  $\alpha \in \mathbb{Q}^\times$ ,  $\alpha \neq \pm 1$ , and assuming the truth of *abc* conjecture,

$$\text{card} \{p \leq x : \alpha^{p-1} \not\equiv 1 \pmod{p^2}\} \gg_\alpha \log x \quad \text{as } x \rightarrow \infty.$$

In [4] Hester Graves and M. Ram Murty extended this result to primes in arithmetical progression by showing that for any  $a \geq 2$  and any fixed  $k \geq 2$ , there are  $\gg \log x / \log \log x$  primes  $p \leq x$  such that  $a^{p-1} \not\equiv 1 \pmod{p^2}$  and  $p \equiv 1 \pmod{k}$ , under the assumption of *abc* conjecture.

In this paper, we study non-Wieferich primes in algebraic number fields. More precisely, we prove the following

**Theorem 1.1.** *Let  $K = \mathbb{Q}(\sqrt{m})$  be a real quadratic field and assume that *abc* conjecture holds in  $K$ . Then there are infinitely many non-Wieferich primes in  $\mathcal{O}_K$  with respect to the unit  $\varepsilon$  satisfying  $|\varepsilon| > 1$ .*

**Theorem 1.2.** *Let  $K$  be any algebraic number field and assume that *abc* conjecture holds in  $K$ . Let  $\eta$  be a unit in  $\mathcal{O}_K$  satisfying  $|\eta| > 1$  and  $|\eta^{(j)}| < 1$  for all  $j \neq 1$ , where  $\eta^{(j)}$  is the  $j$ th conjugate of  $\eta$ . Then there exists infinitely many non-Wieferich primes in  $K$  with respect to the base  $\eta$ .*

The plan of this article is as follows. In section 2, we shall define *abc* conjecture for number fields. In section 3, a brief introduction to Wieferich/non-Wieferich primes over number fields will be given and in section 4 and 5, we shall prove theorem 1.1 and theorem 1.2, respectively.

## 2. THE *abc*-CONJECTURE

The *abc*-conjecture propounded by Oesteré and Masser (1985) states that given any  $\delta > 0$  and positive integers  $a, b, c$  such that  $a + b = c$  with  $(a, b) = 1$ , we have

$$c \ll_{\delta} (\text{rad}(abc))^{1+\delta},$$

where  $\text{rad}(abc) := \prod_{p|abc} p$ .

The *abc* conjecture has several applications, the reader may refer to [6], [7], [8], [9] for details.

To state the analogue of *abc*-conjecture for number fields, we need some preparations, which we do below. The interested reader may refer to [6], [7] for more details.

Let  $K$  be an algebraic number field and let  $V_K$  denote the set of primes on  $K$ , that is, any  $v$  in  $V_K$  is an equivalence class of norm on  $K$  (finite or infinite). Let  $\|x\|_v := N_{K/\mathbb{Q}}(\mathfrak{p})^{-v_{\mathfrak{p}}(x)}$ , if  $v$  is a prime defined by the prime ideal  $\mathfrak{p}$  of the ring of integers  $\mathcal{O}_K$  in  $K$  and  $v_{\mathfrak{p}}$  is the corresponding valuation, where  $N_{K/\mathbb{Q}}$  is the absolute value norm. Let  $\|x\|_v := |g(x)|^e$  for all non-conjugate embeddings  $g : K \rightarrow \mathbb{C}$  with  $e = 1$  if  $g$  is real and  $e = 2$  if  $g$  is complex. Define the height of any triple  $a, b, c \in K^{\times}$  as

$$H_K(a, b, c) := \prod_{v \in V_K} \max(\|a\|_v, \|b\|_v, \|c\|_v),$$

and the radical of  $(a, b, c)$  by

$$\text{rad}_K(abc) := \prod_{\mathfrak{p} \in I_K(a, b, c)} N_{K/\mathbb{Q}}(\mathfrak{p}),$$

where  $I_K(a, b, c)$  is the set of all primes  $\mathfrak{p}$  of  $\mathcal{O}_K$  for which  $\|a\|_v, \|b\|_v, \|c\|_v$  are not equal.

The *abc* conjecture for algebraic number fields is stated as follows: For any  $\delta > 0$ , we have

$$H_K(a, b, c) \ll_{\delta, K} (\text{rad}(a, b, c))^{1+\delta}, \quad (3)$$

for all  $a, b, c \in K^{\times}$  satisfying  $a + b + c = 0$ , the implied constant depends on  $K$  and  $\delta$ .

## 3. WIEFERICH/NON-WIEFERICH PRIMES IN NUMBER FIELDS

Let  $K$  be a algebraic number field and  $\mathcal{O}_K$  be its ring of integers. A prime  $\pi \in \mathcal{O}_K$  is called Wieferich prime with respect to the base  $\varepsilon \in \mathcal{O}_K^*$  if

$$\varepsilon^{N(\pi)-1} \equiv 1 \pmod{\pi^2}, \quad (4)$$

where  $N(\cdot)$  is the absolute value norm. If the congruence (4) does not hold for a prime  $\pi \in \mathcal{O}_K$ , then it is called non-Wieferich prime to the base  $\varepsilon$ .

**Notation:** In what follows,  $\varepsilon$  will denote a unit in  $\mathcal{O}_K$  and we shall write  $\varepsilon^n - 1 = u_n v_n$ , where  $u_n$  is the square free part and  $v_n$  is the squarefull part, i.e., if  $\pi | v_n$  then  $\pi^2 | v_n$ . We shall denote absolute value norm on  $K$  by  $N$ .

## 4. PROOF OF THEOREM (1.1)

Let  $K = \mathbf{Q}(\sqrt{m})$ ,  $m > 0$  be a real quadratic field and  $\mathcal{O}_K$  be its ring of integers. Let  $\varepsilon \in \mathcal{O}_K^*$  be a unit with  $|\varepsilon| > 1$ . The results of Silverman [2], Ram Murty and Hester [4] elucidated in the introduction uses a key lemma of Silverman (Lemma 3, [2]). We derive an analogue of Silverman's lemma for number fields which will play a fundamental role in the proof of the main theorems.

**Lemma 4.1.** *Let  $\mathbf{Q}(\sqrt{m})$  be a real quadratic field. Let  $\varepsilon \in \mathcal{O}_K^*$  be a unit. If  $\varepsilon^n - 1 = u_n v_n$ , then every prime divisor  $\pi$  of  $u_n$  is a non-Wieferich prime with respect to the base  $\varepsilon$ .*

**Proof.** Let us suppose  $\varepsilon^n - 1 = u_n v_n$  for some  $n$ . Then

$$\varepsilon^n = 1 + \pi w, \quad (5)$$

with  $\pi | u_n$  and  $\pi$  and  $w$  are coprime. As  $\pi$  is a prime, we have  $N(\pi) = p$  or  $p^2$ ,  $p$  is a rational prime.

Case (1): Suppose  $N(\pi) = p$ .

From equation (5), we get

$$\varepsilon^{n(p-1)} \equiv 1 + (p-1)\pi w \not\equiv 1 \pmod{\pi^2}.$$

Case (2): Suppose  $N(\pi) = p^2$ .

Again from equation (5), we obtain

$$\varepsilon^{n(p^2-1)} = \varepsilon^{n(N(\pi)-1)} = (1 + \pi w)^{(p^2-1)} \equiv 1 + \pi w(p^2 - 1) \not\equiv 1 \pmod{\pi^2}.$$

Thus in either case,

$$\varepsilon^{(N(\pi)-1)} \not\equiv 1 \pmod{\pi^2},$$

and hence  $\pi$  is a non-Wieferich prime to the base  $\varepsilon$ .  $\square$

The above lemma shows that whenever a prime  $\pi$  divides  $u_n$  for some positive integer  $n$ , then  $\pi$  is a non-Wieferich prime with respect to the base  $\varepsilon$ . Thus, if we can show that the set  $\{N(u_n) : n \in \mathbb{N}\}$  is unbounded, then this will imply that the set  $\{\pi : \pi | u_n, n \in \mathbb{N}\}$  is an infinite set. Consequently, this establishes the fact that there are infinitely many non-Wieferich primes in every real quadratic field with respect to the unit  $\varepsilon$ , with  $|\varepsilon| > 1$ . Therefore, we need only to show the following

**Lemma 4.2.** *Let  $\mathbf{Q}(\sqrt{m})$  be a real quadratic field. Let  $\varepsilon \in \mathcal{O}_K^*$  be a unit with  $|\varepsilon| > 1$ . Then under abc-conjecture for number fields, the set  $\{N(u_n) : n \in \mathbb{N}\}$  is unbounded.*

**Proof.** Invoking abc-conjecture (3) to the equation

$$\varepsilon^n = 1 + u_n v_n \quad (6)$$

yields

$$|\varepsilon^n| \ll \left( \prod_{\mathfrak{p} | u_n v_n} N(\mathfrak{p}) \right)^{1+\delta} \ll (N(u_n) \sqrt{N(v_n)})^{1+\delta} \quad (7)$$

for some  $\delta > 0$ . Here the implied constant depends on  $K$  and  $\delta$ .

Now, as  $|\varepsilon| > 1$ ,

$$N(u_n)N(v_n) = N(\varepsilon^n - 1) < |\varepsilon^n - 1| < 2|\varepsilon|^n,$$

i.e.,

$$N(v_n) < 2|\varepsilon|^n / N(u_n).$$

Substituting the above expression in (7), we obtain

$$|\varepsilon^n| \ll \left( N(u_n) \frac{|\varepsilon|^{n/2}}{\sqrt{N(u_n)}} \right)^{1+\delta}.$$

Thus,

$$|\varepsilon|^{\frac{n(1-\delta)}{2}} \ll (N(u_n))^{\frac{1+\delta}{2}}.$$

Thus, for a fixed  $\delta$ ,  $N(u_n) \rightarrow \infty$  as  $n \rightarrow \infty$ . This proves the lemma and hence completes the proof of the theorem.  $\square$

## 5. NON-WIEFERICH PRIMES IN ALGEBRAIC NUMBER FIELDS

In this section, we generalize the arguments of previous section to arbitrary number fields. From now onwards,  $K$  will always denote an algebraic number field of degree  $[K : \mathbb{Q}]$  over  $\mathbb{Q}$ . Let  $r_1$  and  $r_2$  be the number of real and non-conjugate complex embeddings of  $K$  into  $\mathbb{C}$  respectively, so that  $[K : \mathbb{Q}] = r_1 + 2r_2$ . We begin with an analogue of Lemma (4.1).

**Lemma 5.1.** *Let  $\varepsilon$  be a unit in  $\mathcal{O}_K$ . If  $\varepsilon^n - 1 = u_n v_n$ , then every prime divisor  $\pi$  of  $u_n$  is a non-Wieferich prime with respect to the base  $\varepsilon$ .*

**Proof.** Let  $N(\pi) = p^k$ , where  $p$  is a rational prime and  $k$  is a positive integer. Then

$$\varepsilon^{n(N(\pi)-1)} = \varepsilon^{n(p^k-1)} = (1 + w\pi)^{(p^k-1)} \equiv 1 + (p^k - 1)w\pi \not\equiv 1 \pmod{\pi^2}.$$

This implies  $\varepsilon^{N(\pi)-1} \not\equiv 1 \pmod{\pi^2}$ .

Thus, the lemma shows that  $\pi$  is a non-Wieferich prime to the base  $\varepsilon$  whenever the hypothesis of the lemma is met. Now, under *abc* conjecture for number fields, we show below the existence of infinitely many non-Wieferich primes.

**Lemma 5.2.** *The set  $\{N(u_n) : n \in \mathbb{N}\}$  is unbounded, where  $u_n$ 's are as defined in Lemma (5.1).*

**Proof.** By the hypothesis of the lemma, we have  $\varepsilon^n = 1 + u_n v_n$ , where  $\varepsilon^n, 1, u_n v_n \in K^\times$ . Applying *abc* conjecture for number fields to the above equation, we obtain

$$\prod_{v \in V_K} \max(|u_n v_n|_v, |1|_v, |\varepsilon^n|_v) \ll \left( \prod_{\mathfrak{p} | u_n v_n} N(\mathfrak{p}) \right)^{1+\delta}, \quad (8)$$

for some  $\delta > 0$ .

Note that for the absolute value  $|\cdot|$  in  $V_K$ , we have

$$|\varepsilon^n| \leq \prod_{v \in V_K} \max(|u_n v_n|_v, |1|_v, |\varepsilon^n|_v) \quad (9)$$

and

$$\left( \prod_{\mathfrak{p} | u_n v_n} N(\mathfrak{p}) \right)^{1+\delta} \leq (N(u_n) \sqrt{N(v_n)})^{1+\delta}. \quad (10)$$

Therefore, the equations (8), (9) and (10), yield

$$|\varepsilon^n| \ll (N(u_n) \sqrt{N(v_n)})^{1+\delta}. \quad (11)$$

In the case of real quadratic fields, the unit  $\varepsilon$  satisfies  $|\varepsilon| > 1$  and this information was crucial in proving Theorem 1.1. However, in the case of general number fields, the following result (see Lemma 8.1.5, [3]) comes to our rescue. We state this result as

**Lemma 5.3.** *Let  $E = \{k \in \mathbb{Z} : 1 \leq k \leq r_1 + r_2\}$ . Let  $E = A \cup B$  be a proper partition of  $E$ . There exists a unit  $\eta \in \mathcal{O}_K$  with  $|\eta^{(k)}| < 1$ , for  $k \in A$  and  $|\eta^{(k)}| > 1$ , for  $k \in B$ .*

Taking  $A = \{k : 1 < k \leq r_1 + r_2\}$  and  $B = \{1\}$ , Lemma 5.3 produces a unit  $\eta \in \mathcal{O}_K^*$  such that  $|\eta| > 1$  and  $|\eta^{(k)}| < 1$ , where  $\eta^{(k)}$  denotes the  $k^{\text{th}}$  conjugate of  $\eta$ ,  $k \neq 1$ . Since, every unit satisfies (11), replacing  $\varepsilon$  with  $\eta$  in (11), we obtain

$$|\eta^n| \ll (N(u_n)\sqrt{N(v_n)})^{1+\delta}, \quad (12)$$

where, by abuse of notation, we shall denote  $\eta^n - 1 = u_n v_n$ , with  $u_n$  and  $v_n$  denoting the same quantities as defined earlier.

Now,

$$N(u_n)N(v_n) = N(\eta^n - 1) = (\eta^n - 1)(\eta^{(2)n} - 1)(\eta^{(3)n} - 1) \cdots (\eta^{(l)n} - 1),$$

where  $l = [K : \mathbb{Q}]$  (say). By Lemma 5.3,  $|\eta^{(j)n} - 1| < 2$  for all  $j, 2 \leq j \leq l$ .

Thus,

$$N(u_n)N(v_n) < C|\eta^n| \quad \text{or} \quad N(v_n) < C|\eta^n|/N(u_n).$$

Now, (12) can be written as

$$|\eta|^{n\frac{1-\delta}{2}} \ll (N(u_n))^{\frac{1+\delta}{2}}$$

or

$$N(u_n) \gg |\eta|^{n\frac{1-\delta}{1+\delta}}. \quad (13)$$

For a fixed  $\delta$ , the right hand side of (13) tends to  $\infty$  as  $n \rightarrow \infty$ . Therefore the set  $\{N(u_n) : n \in \mathbb{N}\}$  is unbounded. This shows that there are infinitely many non-Wieferich primes in  $K$  with respect to the base  $\eta$ .  $\square$

### Acknowledgement

The authors express their indebtedness to Prof. M. Ram Murty for some important discussions. The second author would like to thank Prof. T.R. Ramadas for encouragement and also acknowledges with thanks for financial support extended by DST through his J.C. Bose Fellowship.

### REFERENCES

- [1] A. Wieferich, *Zum Letzten Fermat'schen Theorem*, J. Reine Angew. Math. 136, (1909), 293-302.
- [2] J.H. Silverman, *Wieferich's criterion and the abc-conjecture*, J. Number Theory 30 (1988) no. 2, 226-237.
- [3] Jody Esmonde, M.Ram Murty, *Problems in Algebraic Number Theory*, Graduate texts in Mathematics, Springer-Verlag New York, Inc.
- [4] Hester Graves, M.Ram Murty, *The abc conjecture and non-Wieferich primes in arithmetic progressions*, J. Number Theory 133 (2013) 1809-1813.
- [5] Daniel A. Marcus, *Number Fields*, Graduate texts in mathematics, 1977, Springer-Verlag.
- [6] Paul Vojta, *Diophantine approximations and value distribution theory*, Lecture Notes in mathematics (1980), Springer-Verlag.
- [7] K. Györy, *On the abc conjecture in algebraic number fields*, Acta Arith. 133 (2008), no. 3, 281-295.
- [8] Abderrahmane Nitaj, [http : //www.math.unicaen.fr/ nitaj/abc.html](http://www.math.unicaen.fr/nitaj/abc.html), A abc conjecture website.
- [9] Murty, M.Ram, *The ABC conjecture and exponents of class groups of quadratic fields*, Murty, V. Kumar (ed.) et al., Number theory. Proceedings of the international conference on discrete mathematics and number theory, Tiruchirapalli, India, January 3-6, 1996 on the occasion of the 100th anniversary of the Ramanujan Mathematical Society. Providence, RI: American Mathematical Society. Contemp. Math. 210, 85-95 (1998)
- [10] PrimeGrid Project, [http : //www.primegrid.com/](http://www.primegrid.com/)

INSTITUTE OF MATHEMATICAL SCIENCES, CIT CAMPUS, TARAMANI, CHENNAI 600 113, INDIA

CHENNAI MATHEMATICAL INSTITUTE, SIPCOT IT PARK, SIRUSERI, CHENNAI 603 103, INDIA

E-mail address, Kotyada Srinivas: [srini@imsc.res.in](mailto:srini@imsc.res.in)

E-mail address, Subramani Muthukrishnan: [subramani@cmi.ac.in](mailto:subramani@cmi.ac.in)